**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

GLOBERANGER CORPORATION	**§**	
	§	
Plaintiff,	**§**	
	§	
v.	**§**	**CIVIL ACTION NO. 3:11-cv-403-B**
	§	
SOFTWARE AG, SOFTWARE AG USA, INC., NANIQ SYSTEMS, LLC and MAIN SAIL LLC,	**§**	
	§	
	§	
	§	
Defendants.	**§**	

SECOND AMENDED COMPLAINT

Plaintiff GlobeRanger Corporation ("GlobeRanger" or "Plaintiff") files this Second Amended Complaint against Software AG ("Software AG – Germany"),[1] Software AG USA, Inc. ("Software AG - USA"), Software AG, Inc. (Software AG – USA and Software AG, Inc., collectively, the "U.S. Subs")(Software AG Germany and the U.S. Subs are collectively referred to herein as, "Software AG"), Naniq Systems, LLC ("Naniq") and Main Sail LLC ("Main Sail") (collectively, "Defendants") and, in support thereof, would respectfully show the Court the matters set forth below.

I. PRELIMINARY STATEMENT

GlobeRanger, a small start-up company, poured a decade of work and tens of millions of dollars into developing technology that is truly transformative and promised to exponentially facilitate the flow of goods and information throughout the world. Software AG, the second largest software vendor in Germany with over $1 billion in yearly revenues, stood to make

[1] Software AG – Germany was dismissed from this lawsuit on April 12, 2013. *See* Doc. 71. Its inclusion in this Second Amended Complaint is for the sole purpose of preserving appeal of issues related to the dismissal.

hundreds of millions of dollars in profit if it could develop this technology. But despite all of Software AG's resources, Software AG had failed where GlobeRanger had succeeded.

Software AG set out to steal GlobeRanger's proprietary and trade secret technology. Naniq and Main Sail offered Software AG access to GlobeRanger's technology, motivated by the prospect of making tens of millions in support contracts once Software AG succeeded.

GlobeRanger achieved the American dream – after ten years of hard work, it had developed technology that promises to cause a quantum leap in how our world functions. Main Sail and Naniq had the means – they learned of the GlobeRanger technology when they supplied support to GlobeRanger customers. Software AG had an irresistible motive: it stood to make hundreds of millions of dollars from stealing GlobeRanger's technology and attaching it to a product already deployed in tens of thousands of companies worldwide. The Defendants obtained a copy of the software and installed an image of the program and the data at one live site onto a laptop. Under false pretenses, Defendants obtained license keys to unlock the software and the data dictionary to enable them to look at the data files and workflows and how they were interrelated. From this information Defendants were then able to discover GlobeRanger's trade secrets and falsely claim that they were developing the technology on their own.

The Defendants attitude towards stealing a decade of GlobeRanger's work was malicious and cavalier. In fact, their co-conspirator laughed about Defendants' misappropriation of GlobeRanger's technology when he confirmed the theft on tape.

II. **PARTIES**

1. Plaintiff GlobeRanger is a corporation organized under the laws of the State of Delaware with its principal place of business in Richardson, Dallas County, Texas.

2. Defendant Software AG – Germany is a German corporation with its principal place of business at Uhlandstrasse 12, 64297 Darmstadt, Germany. Software AG – Germany has

been served and has appeared in this action. Software AG – Germany was dismissed from this action on April 12, 2013 by order of the Court.

3. Defendant Software AG - USA is a corporation organized under the laws of Delaware with its principal place of business at 11700 Plaza America Drive, Suite 700, Reston, Virginia 20191-4751. Software AG - USA has been served and has appeared in this action.

4. Defendant Software AG, Inc. is a corporation organized under the laws of Virginia with its principal place of business at 11700 Plaza America Drive, Suite 700, Reston, Virginia 20191-4751. Software AG, Inc. has been served and has appeared in this action.

5. Defendant Naniq is a limited liability company organized under the laws of the State of Alaska with its principal place of business at 2121 Abbott Road Anchorage, Alaska 99507-4453. Naniq has been served and has appeared in this action.

6. Defendant Main Sail is a limited liability company organized under the laws of the State of Ohio with its principal place of business at 20820 Chagrin Blvd, Suite 201, Cleveland, Ohio 44122. Main Sail has been served and has appeared in this action.

III. <u>JURISDICTION AND VENUE</u>

7. This Court has jurisdiction as the amount in controversy is above the minimum jurisdictional limits of this Court.

8. The Court has personal jurisdiction over the U.S. Subs and Naniq because each of them maintains an office in and regularly conducts business within the State of Texas and has committed acts within the State of Texas giving rise to this action. The Court has personal jurisdiction over Main Sail because it regularly conducts business within the State of Texas.

9. The Court has personal jurisdiction over Software AG – Germany because Software AG – Germany and/or one of its co-conspirators has engaged in tortious conduct

against GlobeRanger in the State of Texas. Further, the Court has personal jurisdiction over Software AG – Germany because the U.S. Subs and Software AG - Germany are a unitary business operation. Further, the Court has personal jurisdiction over Software AG – Germany because the U.S. Subs are wholly owned by Software AG – Germany, are financially dependent on Software AG – Germany and Software AG – Germany consolidates the U.S. Subs' financials. Software AG – Germany selects and assigns the U.S. Subs' key personnel and controls the operations of the U.S. Subs, including the U.S. Subs sales & marketing and product development, which are the core issues of this lawsuit. Further, the Court has personal jurisdiction over Software AG – Germany because the U.S. Subs engage in purposeful activities in Texas including maintaining several offices, a large workforce, providing products and services to Texas residents, and entering into contracts with Texas residents. The U.S. Subs' continuous and systematic contacts with the forum exist for the benefit of Software AG – Germany, Software AG – Germany exercises control over the U.S. Subs' purposeful activities, and these activities are sufficiently important to Software AG – Germany that if it did not have the U.S. Subs to perform them, Software AG's own officials would undertake to perform substantially similar activities. Further, the Court has personal jurisdiction over Software AG – Germany because Software AG – Germany participated in a conspiracy to defraud, misappropriate trade secrets, engage in unfair competition, and tortiously interfere with GlobeRanger's contracts and prospective business relations. Software AG – Germany and/or its co-conspirators committed one or more overt acts in furtherance of the conspiracy in Texas.

10. Each of the Defendants has established minimum contacts with the forum such that the exercise of jurisdiction over each of the Defendants would not offend traditional notions of fair play and substantial justice.

11. Venue is proper in the Northern District of Texas pursuant to 28 U.S.C. § 1391 because Defendants are subject to personal jurisdiction in the Northern District of Texas and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred within this district and division.

IV. BACKGROUND

A. RFID Technology.

12. Imagine you are Imagine pushing your fully loaded grocery cart through a doorway and walking straight to your car; no waiting in line; no pulling out every last product and placing it on the conveyor belt; no standing there listening to the repetitive beep of each item being passed over the scanner; no struggling to get the bar code positioned over the red light on the scanner "just so;" and no feeling of despair when the register comes up with "SKU not found." And because of a special card or the mobile phone in your pocket, you do not even have to pull out your credit card to pay. Just pick up your groceries and take them straight home.

13. Now imagine you are the owner of the grocery store. As customers pick products off the shelves, the information is sent directly to store's inventory system. The store's inventory system automatically notifies the distribution center. The data is automatically adjusted for recent trends and seasonality and orders are instantly placed with the vendor as inventory is sold. This automatic system even determines how ever-changing freight charges and weather impact the choice of truck, train, and route.

14. This transformative technology starts with tags and readers known as radio frequency identification ("RFID"), but requires the perfect combination of software, business processes, and system architecture (the "RFID System") to link the RFID System with an enterprise's existing information technology ("IT") systems.

15. To work seamlessly throughout an enterprise and at all points of the intake and distribution channels, an RFID System requires the design of business processes (the "Business Processes"). The Business Processes are the "secret sauce" necessary to make the software and hardware components of RFID work in harmony. RFID tags and readers provide automatic acknowledgement that "something" has crossed the reader, but the Business Processes and software associated with those Business Processes tell the RFID System how to recognize what the "something" is, where it came from, where it is going, how long it took to get there, and most importantly, what the RFID System should do about it.

16. Once an RFID reader, RFID tags, and Business Processes are in place, an RFID System is created. But an RFID System in a vacuum ignores the true power of RFID – tying an enterprise's inventory, ordering, shipping, and other existing IT such that there exists automatic, seamless, and enterprise-wide architecture (the "Architecture"). The Architecture is the blueprint for how the RFID System will be implemented and maintained in the context of the larger enterprise. Finally, industry and company-specific issues must be considered and accommodated. Changes or additions in software, hardware, and Business Process (the "Solution") contribute to form the end-to-end system.

17. RFID itself is not new technology. Retailers have used large, bulky, and expensive RFID tags for theft detection for years. If a tag crosses through a detector at the front of a store, an alarm sounds. To take RFID to the next level, the tag needed to be smaller and cheaper. The most expensive and bulky part of these historical tags was a battery inside the tag that powered the communications. These battery-powered tags are called "active" RFID tags.

18. Microchip advancement eventually allowed for the development of cost-effective "passive" RFID tags, which use radio frequency energy transferred from the reader to the tag to

power the tag. Even then more development was needed. A dolly full of products tagged with passive RFID tags could be passed through a reader and broadcast, but an RFID System was needed to listen, interpret, and react.

19. Enormous resources are required to develop an RFID System. It is also extraordinarily difficult. In the past, only companies such as Wal-Mart have had the resources to develop true passive RFID Systems. It took it years. In fact, it was only very recently – August 2010 – that Wal-Mart moved from merely tagging pallets of product and shipping containers to a pilot program of placing passive RFID tags on men's jeans.

20. Wal-Mart has RFID Systems made by and for Wal-Mart. Like a bespoke suit, it is not going to fit other enterprises or industries. But what would happen if someone developed passive RFID Systems that could be dropped in and customized to any enterprise, in any industry? The engineers who formed GlobeRanger set out to do just that.

B. <u>GlobeRanger Invests in RFID Technology Research and Development</u>.

21. In 1999, GlobeRanger was formed with the singular purpose of advancing RFID technology. It would be risky, expensive, and difficult, but the employees and investors in GlobeRanger took the gamble, made the sacrifices, and did the work – a decade of work.

22. First, GlobeRanger developed its own RFID software platform – iMotion. iMotion was deployed across multiple industries, including retail, government, healthcare, and perishables supply chains. If a user opens a box of iMotion software, loads it a computer, and runs the program, he will not have an RFID System. He needs hardware – passive RFID tags, a reader, and a server. He needs Business Processes to translate what is happening in the real world. He needs Architecture to link up with existing IT infrastructure. He needs to deploy. Adopting each component piecemeal flies in the face of the holistic purpose of an RFID System.

23. Every industry, indeed every organization's, optimal RFID System is different. How many readers? Where should they be installed? What products should be tagged? Where are the bottlenecks? Drawing on years of experience seeing the different ways in which the iMotion platform was incorporated into an RFID System and deployed in a wide variety of contexts, GlobeRanger sought to develop a true end-to-end solution that could be adapted to different business processes, depending on the customer (the "GlobeRanger's RFID Solution").

24. In the end, this initial piecemeal approach was a good thing. Since GlobeRanger developed iMotion with the knowledge that it would have to be adapted to hardware, technology, and legacy IT systems developed by multiple parties, GlobeRanger engineers were adept at making things scalable and adaptable.

25. The GlobeRanger RFID Solution is a true chameleon, and can be quickly adapted to suit any customer's needs. The GlobeRanger RFID Solution is used to track crime scene evidence in Holland. The GlobeRanger RFID Solution monitors the removal of hazardous materials from a nuclear site in Tennessee. The GlobeRanger RFID Solution knows just where "your dollop of Daisy" sour cream is between farm and market. The GlobeRanger RFID Solution at a Wal-Mart vendor even works in concert with Wal-Mart's bespoke internal RFID Systems.

26. In fact, the GlobeRanger's RFID Solution is so flexible and versatile, GlobeRanger can take its RFID Solution and adapt and deploy it within an enterprise – any enterprise – within 60 to 90 days.

27. The GlobeRanger RFID Solution had such a competitive advantage, that, prior to 2008, GlobeRanger had virtually no real competitors in the passive RFID market – particularly

in an industry that had the wherewithal and desire to implement RFID on a massive scale: government.

C. The Department of Defense's 2004 RFID Mandate.

28. In 2004, the United States Department of Defense ("DOD") issued a mandate for each of its agencies and military services to implement passive RFID technology. The mandate was unfunded, which meant that contractor selections and implementation would be made at the agency level and by each respective military branch.

29. Once GlobeRanger achieved success with the GlobeRanger RFID Solution and the branches of the military and DOD agencies began to allocate funds to comply with the passive RFID mandate, GlobeRanger obtained several agency and military service branch contracts. GlobeRanger is now the enterprise standard for the Defense Logistics Agency. GlobeRanger is the enterprise standard for the entire Air Force. GlobeRanger won contracts from the U.S. Marine Corp, the Army, and was quickly deployed to initial sites.

30. GlobeRanger was a resounding success throughout the DOD. It had an adaptable system that could be quickly customized. GlobeRanger proved that the GlobeRanger RFID Solution was not just a chameleon that could move from tracking a murder weapon to monitoring fish, the GlobeRanger RFID Solution could communicate with and among the highly specialized and varied existing IT systems used by the U.S. military and defense agencies. GlobeRanger's decade-long investment in RFID technology began to pay off.

D. Software AG Does Not Have Commercial RFID Solution.

31. Software AG is a leading provider of business process management with over $1 billion in annual revenues.

32. As companies and their IT systems have become complex and multi-layered, they have increasingly turned towards enterprise consolidation. In 2007, webMethods, a company that marketed a platform for enterprise consolidation by the same name, had a dominant market position. WebMethods is middleware. Middleware is a communication subsystem between two or more enterprise systems that moves data back and forth. For example, if a company seeks to more efficiently and accurately target its marketing, middleware can be used to make its customer database exchange information with its ordering system. Middleware is a base – like a personal computer's operating system. Like iMotion, a user cannot open a box and install webMethods and expect seamless communication with existing IT systems. Rather, to make webMethods work with the existing systems, consultants provide business process management services to develop a tailored solution. Like GlobeRanger, webMethods consultants learned, over time, the most optimal way to incorporate webMethods into a retailer, a health care company, a government agency, and a wide variety of other enterprises.

33. In April 2007, Software AG purchased webMethods for more than *a half a billion dollars*. WebMethods was worth so much because it is literally everywhere – in every industry, every sized enterprise. WebMethods consultants had a deep bench of experience developing business processes and layering solutions on top of webMethods across these enterprises. Given the widespread use of webMethods, if Software AG could develop additional solutions to layer on top of the webMethods base, Software AG had an enormous built-in market just from the existing webMethods and business process management client base.

34. RFID is the Holy Grail solution to add to the webMethods platform. At the time of the acquisition, webMethods solutions had been developed for virtually every type of enterprise. If Software AG could add an RFID solution to webMethods, Software AG would hit

a massive home run – making hundreds of millions of dollars from its business process management services. RFID was an incredible opportunity to maximize returns on its half a billion-dollar acquisition.

35. But even with this incredible opportunity, even with Software AG's near-limitless resources, a year after the acquisition, Software AG did not have an RFID Solution on the market.

36. GlobeRanger purposefully made the GlobeRanger RFID Solution adaptable and customizable to suit a given enterprise's needs. Its platform, iMotion, was developed specifically for RFID and adapted easily to new business process, architecture, and deployments. GlobeRanger made a chameleon, an RFID Solution that could be dropped in anywhere, anytime. Development was difficult and costly – GlobeRanger invested over a decade of research and development and tens of millions of dollars to develop its versatile RFID Solution.

37. Conversely, Software AG's platform, webMethods, was not developed for RFID. Rather, RFID was an afterthought. It did not adapt easily to RFID business processes, architecture, and deployments. Software AG had to not only create an RFID Solution, it needed an RFID Solution that worked with the webMethods platform if it was going to take advantage of the captive market of webMethods clients.

38. Software AG's acquisition of webMethods occurred in April 2007. That meant Software AG had years of research and development ahead of it before it would have a working RFID Solution. Software AG had just spent a half a billion dollars. It had to show returns on this investment. Software AG decided that it would develop an RFID Solution through corporate espionage.

E. **Naniq and Main Sail Gain Access to GlobeRanger's RFID Solution and Sign GlobeRanger's End User Agreement.**

39. The DOD mandate for the implementation of RFID was an "unfunded mandate." The significance of a mandate being unfunded is that contractors vie for many small to medium contracts at the agency and military service branch level, and contracts are funded out of general funds at these levels.

40. As the various customers that make up the DOD awarded their passive RFID contracts, GlobeRanger stood alone, winning Defense Logistics Agency, Air Force, Marine, Army, and Navy contracts. No competitor was in a position to catch up. If the barriers to entry to the passive RFID market are many, the barriers to entry for the government passive RFID contracts are nearly insurmountable. In addition to the considerable technical challenges, there is a very long, very slow pay off for government contracts. There are months or even years of working on the pursuit, presenting up the chain of command, and then months or even years of pilot programs and testing. The reward is often multi-year contracts that require considerable upfront investment before returns are achieved.

41. Defendant Main Sail is a services company. It re-sells third-party software, consults, and provides IT service support. Main Sail does not research, develop, or produce technology.

42. Main Sail learned of GlobeRanger and its transformative technology in late 2005 when GlobeRanger and Main Sail worked on a project for the implementation of passive RFID at the Navy's Bangor, Maine site. Jack Rhyne, from Main Sail, was involved in the Bangor RFID implementation project. GlobeRanger set up a server at Bangor with its iMotion software, and in early 2006, GlobeRanger went live, tracking the provisions to and from nuclear submarines. It was a resounding success.

43. Defendant Naniq is also a services company. It re-sells third-party software, consults, and provides IT service support. Naniq does not research, develop, or produce technology.

44. In 2007, Kim Gray, who serves as the Director of Defendant Naniq, worked with GlobeRanger on a Defense Logistics Agency project in Alaska, which was another GlobeRanger success.

45. GlobeRanger continued its dominance in the DOD. In 2006, the DLA and adopted GlobeRanger across the board. The Air Force began substantial deployments of a GlobeRanger RFID Solution (the Air Force would also adopt GlobeRanger enterprise-wide as of 2009). The Army and the Marine Corps awarded development contracts, and GlobeRanger began deployments at Army and Marine Corps. All of these deployments were done in the midst of two wars. When it came to seamless integration of RFID technology to get supplies to our troops on the front line, the DOD trusted GlobeRanger.

46. GlobeRanger also began to roll out the GlobeRanger RFID Solution adapted specifically for the Navy (the "GlobeRanger Navy Solution"). The Navy contract would be by far the largest client at the DOD. The Navy has more than 700 worldwide sites. The Navy intended to use passive RFID to facilitate the supplying of these sites, the shipment of materials to war zones, and the loading and unloading of city-size aircraft carriers. The GlobeRanger Navy Solution was initially deployed at six Navy sites and received multiple commendations for its immediate success.

47. The Navy's passive RFID program was directed from Naval Supply's Automatic Identification Technology office ("Navy AIT"). Navy AIT Project Manager Bob Bacon was in charge of the program. As the Navy's passive RFID program progressed, a small player, Naniq,

began to gain considerable influence over Bob Bacon, who awarded a contract to Naniq to provide IT support at the initial Navy-GlobeRanger sites.

F. The Navy Requests New RFID Architecture.

48. In July of 2008, the Navy AIT planned to implement Enterprise Resource Planning – or ERP. As part of its next generation, or NGEN (next generation) project, the Navy planned to modernize its kaleidoscope of IT under an ERP Solution.

49. The Navy's Naval Supply ("NAVSUP") Chief Information Officer had thought ahead as to how this future implementation of ERP would affect existing programs. The Navy's RFID system needed to be able to support both the Navy's legacy IT systems and transition to a new ERP Solution, such as Oracle and SAP, in the future. This is exactly what the GlobeRanger RFID Solution did best – it could be adapted to any environment.

50. The introduction of ERP meant that the Architecture of the GlobeRanger RFID Solution needed to be revamped. GlobeRanger undertook three months of research and development and concomitant sleepless nights, testing, reviewing, and preparing a deck (PowerPoint presentation) to present to the Navy. Once the go-ahead was given on the new Architecture, GlobeRanger was prepared to begin rolling out deployments to the Navy's 700 sites within 60-90 days.

51. In August of 2008, GlobeRanger traveled to Navy AIT to present the results to Bob Bacon. A copy of the briefing was given to Bob Bacon and to the two prime contractors for the Navy IT, CACI and SAIC. After the presentation, GlobeRanger was expected to present up the chain of command to the Navy's NAVSUP Chief Information Officer. But the NAVSUP meeting never happened.

52. For ten years, GlobeRanger and its employees were singularly focused on perfecting cutting-edge, transformative RFID technology for its customers. In August 2008, they were the star of the DOD's passive RFID mandate and on the cusp of its largest opportunity to date – the Navy contract. But then, GlobeRanger found itself in the midst of a civil conspiracy that involved sex, lies, and an audiotape.

G. Defendants Procure Navy Contracts Through Improper Influence.

53. Kim Gray at Naniq was unusually successful at winning Navy AIT contracts for Naniq. She was also having an improper relationship with Bob Bacon, the married head of Navy AIT.

54. Just a week after GlobeRanger presented its research for a new Architecture to Bob Bacon and handed Bob Bacon a copy of their presentation, Kim Gray from Naniq and Jack Rhyne from Main Sail, two companies that re-sold third party software and provided help lines for day-to-day support of systems built and deployed by others, were inexplicably in possession of an RFID system Architecture for one of the most complex enterprises in the world – the United States Navy.

55. Despite the fact that GlobeRanger was deployed with massive success across the DOD, Naniq and Main Sail, with the knowledge and consent of Bob Bacon, instead turned to Software AG, who did not even have a commercial RFID Solution at the time, to build the system under "their" Architecture.

56. In February of 2009, a year and a half after the webMethods acquisition, Software AG still did not have an RFID application for webMethods.

57. At the same time, American companies, such as Wal-Mart and Target, were actively implementing RFID solutions. Moreover, the American military – through

GlobeRanger – had RFID technology adapted for military use deploying throughout the Department of Defense. The German government was determined to not let its private and military sectors fall behind. Illustrating how critical RFID technology is becoming to world commerce and military readiness, the German government created and funded ADiWa (Allianz Digitaler Warenfluss).

58. ADiWa is a research consortium that includes the two largest software companies in Germany, SAP and Software AG, as well as academics and various military and civil agencies of the German government. The ADiWa website explains that the purpose of the public-private consortium is to "fill in the gaps of knowledge" in order to closely integrate objects and products into business processes through RFID-tagged products.

59. Software AG boasts of its involvement in ADiWa on the Software AG website. It describes Software AG's main contribution to the ADiWa consortium as "RFID applications."

60. On February 2, 2009, Software AG – Germany's Chief Product Officer and Executive Committee member, Dr. Peter Kürpick, was on hand to receive the German government's notice of approval for ADiWa. As Chief Product Officer, Dr. Kürpick was in charge of Software AG's blockbuster product webMethods. He already had a mandate from the company to develop and commercialize an RFID solution that would work with webMethods. Now he had even more pressure – a mandate from the German government to contribute RFID solutions to the ADiWa consortium.

61. Just a few months later, in May of 2009, Software AG stepped from the shadows to pursue a contract from Navy AIT to develop an RFID solution for the Navy, with Naniq and Main Sail's support. Software AG was not even close to developing an RFID Solution at the time. In press releases from 2009, Software AG tells prospective clients it was envisioning the

future development of passive RFID for 40 foot by 10 foot shipping containers. Meanwhile, at the same time, GlobeRanger's RFID Solution was able to track an order of 10,000 individual products within a container and report the location of each in the supply chain from the warehouse in the United States to the soldier in Afghanistan. Software AG was years behind GlobeRanger. And yet in May of 2009, Bob Bacon issued the Navy AIT purchase order to Software AG.

62. For Software AG, this initial purchase order was less about the money to be earned from the US Navy. It was more about the opportunity to be gained – an opportunity to commit the theft of GlobeRanger's RFID Solution.

63. The harm that came from the improper influence of Defendants over Navy AIT was not just harm to GlobeRanger. GlobeRanger had a passive RFID product. GlobeRanger had an RFID Solution for the Navy. GlobeRanger had been successfully tested at six Navy sites. GlobeRanger had the specialized knowledge it would take to deploy at 700 Navy sites around the world within 60-90 days. Despite these qualifications, despite the fact that the country is in the midst of *two wars*, Software AG, with no passive RFID solution, let alone a Navy solution, with no testing, and no ability to quickly deploy, ended up with a vital role in national security.

64. The U.S. Subs are the sales and marketing representatives of Software AG – Germany in the United States. The U.S. Subs exist and conduct their activities solely for the benefit of Software AG – Germany. The U.S. Subs' operations are controlled by Software AG – Germany. Software AG centralized its global products line under the Chief Product Officer in Germany, Dr. Peter Kürpick. Software AG centralized its research and development under its Chief Technology Officer in Germany. Together with Software AG – Germany's executive

board, strategy, sales, marketing, research and development of webMethods and an RFID solution is directed and controlled by Software AG – Germany.

65. These same centralized heads of products and research and development were actively involved with ADiWa, and dealt directly with ADiWa's corporate, civil governmental and military governmental participants in Germany.

66. GlobeRanger's RFID Solution, adapted for U.S. military use, was exported to Germany and has been or will be handed over to SAP, the German government, the German military, and any other government, military, or corporation that these parties decide to sell it to.

67. In any event, Kim Gray's relationship with Bob Bacon did not end well. Bob Bacon apparently subjected Kim Gray to harassment; perhaps the change of heart resulted from his discovery of the Software AG relationship. Kim Gray sought protection from the authorities. The Navy placed Bob Bacon on administrative leave.

H. **Defendants Misappropriate GlobeRanger Technology.**

68. Before Kim Gray's relationship with Bob Bacon soured, he set up a special lab at Navy AIT in Mechanicsburg, Pennsylvania. Software AG, Naniq, and Main Sail began to work together in the lab, ostensibly on the RFID solution that Software AG had contracted to develop for the Navy.

69. Secreted away in the lab with the other co-conspirators, Software AG set out to develop a passive RFID Solution that would work with its webMethods platform. Software AG was at point zero. Software AG had no RFID solution when it obtained the Navy contract in May of 2009. It had taken GlobeRanger a decade to develop the GlobeRanger RFID Solution. Yet Software AG had, incredibly, agreed to develop its own in a matter of months. Software

AG thought it could make this timeline because it had already agreed with Naniq, Main Sail, and Bob Bacon to steal the GlobeRanger RFID Solution.

70. Software AG sought to use webMethods, presumably to realize a return on its half billion-dollar acquisition. But webMethods was fickle, and it was not developed for RFID like GlobeRanger's iMotion platform. It had taken GlobeRanger a decade to develop iMotion. But again, Software AG had preternatural confidence in its ability to transform webMethods into an RFID platform. The preternatural confidence came from its agreement with Naniq, Main Sail, and Bob Bacon to obtain illegal access to peer inside of GlobeRanger's iMotion platform.

71. The Defendants obtained access to the GlobeRanger RFID Solution through a series of lies. On August 12, 2009, the Defendants caused Bob Bacon to request iMotion license keys subject to GlobeRanger's EULA, ostensibly for support of existing Navy-GlobeRanger sites. This was a false pretense.

72. In reliance upon the representations that the license keys would be used for a lawful purpose and in accordance with GlobeRanger's EULA, GlobeRanger provided the iMotion license keys. GlobeRanger was not, however, without its suspicions.

73. On August 30, 2009, GlobeRanger sent a letter to Naniq reminding it that: (i) the use of any GlobeRanger license keys or software shall be limited to the direct support of Navy AIT's existing installation of GlobeRanger software and for no other purpose and otherwise subject to the terms of the GlobeRanger EULA, which is attached hereto as **Exhibit A** and incorporated by reference; and (ii) upon the termination of Naniq's support contract with respect to Navy AIT's installation, Naniq shall return, delete or destroy all such software and related materials, and so certify to GlobeRanger. Naniq did not respond.

74. Naniq, through its support contract for Kaneohe Bay, a GlobeRanger Navy site, had access to the GlobeRanger Navy Solution at that location (the "K-Bay Solution"). GlobeRanger subsequently discovered that Defendants and their co-conspirator, Bob Bacon, loaded a copy of the K-Bay Solution on a laptop, in violation of the GlobeRanger EULA.

75. While copying an image of the K-Bay Solution onto an unauthorized laptop is technically possible, the image itself is useless. GlobeRanger had protections against access to its confidential and trade secret information. The image of the K-Bay Solution was useless without an iMotion license key. License keys are server-specific, and cannot be transferred from one server to another.

76. As described above, through the Defendants' August 12, 2009 lie, Defendants circumvented these additional protections by acquiring the iMotion license keys under false pretenses. Once the license key was installed, the K-Bay Solution went live on the laptop. Defendants did not just have a copy of iMotion to look at, they had stolen and lied their way into having access to a live, customized GlobeRanger RFID Solution. Defendants could peer at the Business Processes, see the solution's architecture and see how it was deployed at a specific site.

77. The extraction of GlobeRanger's trade secret and confidential information continued unabated for several months. At this point, the GlobeRanger Navy Solution could have been deployed enterprise-wide across the Navy. The Defendants had caused the money that should have gone to GlobeRanger Navy deployments to be misdirected to Software AG.

78. Software AG, a large German corporation, was receiving a U.S. government subsidy to steal technology from a U.S. company and supply it to the German military, civil, and corporate members of the ADiWa consortium. With this subsidy and at the expense of the impact their actions on U.S. troops fighting two wars, Software AG would make hundreds of

millions of dollars. For their participation, Naniq and Main Sail will be awarded with millions of dollars in support contracts and potentially tens of millions of dollars in re-seller licenses and support licenses from Software AG.

79. In January 2010, another lie resulted in the acquisition of GlobeRanger trade secrets. Bob Bacon, on behalf of Defendants, falsely represented that Navy AIT required GlobeRanger's data dictionary, again ostensibly for support of GlobeRanger sites. A data dictionary allows a system designer to understand the fields of meta-data in a system. GlobeRanger, in reliance on the representations of Bob Bacon, sent portions of the data dictionary.

80. Defendants then not only had access to GlobeRanger's K-Bay Solution, but they had also had gained unlawful access to GlobeRanger's data dictionary and workflows, information that would tell Defendants how the GlobeRanger Navy Solution and GlobeRanger's iMotion middleware were interrelated. As shown by the passages of many months since they obtained their unlawful access to the K-Bay Solution, Software AG could not simply copy the software and start rolling out at Naval Bases around the world. Software AG needed months to misappropriate the entire GlobeRanger RFID Solution - the complex Architecture, the Business Processes, and how it was deployed in a real world setting. Defendants had access to the sites where GlobeRanger was installed. Defendants could see how GlobeRanger went about actually deploying on site, how it set up its readers, how it tagged its product, how it incorporated business processes into the design of the warehouse, and how it had trained the sailors.

81. Defendants used this improperly procured information to set up their lab. Defendants installed an RFID reader, tagged product, and hooked it up to the GlobeRanger iMotion server. Software AG could now poke and prod at will. As a result of their improper and

indeed unlawful acquisition of GlobeRanger's trade secret information Defendants took a giant leap, and began to test a Software AG Navy solution that included webMethods middleware.

82. Software AG did not have an RFID product in May of 2009. It took GlobeRanger a decade and tens of millions of dollars to create their RFID System. It took Defendants, cooperating in a conspiracy to misappropriate GlobeRanger's RFID Solution, just one tenth of the time – a 10x head start. And the Defendants had tricked the U.S. government, the U.S. taxpayers, into paying for it.

83. In April of 2010, GlobeRanger's worst fears were confirmed: its decade of work, its ultra-dominant position in the government market, its chameleon-like RFID Solution that had the promise of becoming the next half a billion dollar acquisition target of a multi-national corporation, had all been stolen.

I. <u>Defendant's Co-Conspirator Admits to the Misappropriation in a Public Forum</u>.

84. On April 16, 2010, Bob Bacon participated in a panel discussion with other DOD personnel at an annual RFID conference. It was no secret that Software AG had never successfully developed an RFID solution for webMethods – unbelievably, the Navy, which needed this system to support wars in Afghanistan and Iraq, had offered to be Software AG's guinea pig. Given the absence of any track record for Software AG and the enormous stakes for the troops deployed overseas to get this right, Bob Bacon was asked how webMethods could even be trusted to properly translate each reading of each tag to the Navy's complicated existing IT systems. Bob Bacon's answer shocked several people in the room.

> *Unidentified speaker*: The question is can [the Navy] trust webMethod's performance between the reads and the business systems?
>
> *Bob Bacon*: We had a jump start because we had already…implemented [the other sites] using GlobeRanger servers on every site. So, we sort of had that in our hip pockets which helped us jump start webMethods because ***we just reverse engineered code from GlobeRanger*** - which saved us... (emphasis added)

85. After that statement, there was laughter from Bob Bacon and a few individuals, and exclamations of surprise from others. Government contractors do not like the idea of having their technology stolen by their peers. One of the meeting's attendees quickly handed the recording over to GlobeRanger.

86. While Kim Gray's relationship with Bob Bacon eventually ended, her relationship with Software AG has been solidified and strengthened. They are now actively marketing the Defendants' cooperation on the Navy RFID program to the commercial sector.

87. In April 2010 – shortly after the Defendants' co-conspirator was caught on tape admitting the theft – Software AG sponsored the 2010 Supply Chain Summit in Dallas, Texas. Software AG and Kim Gray told attendees, who were customers, potential customers, and market peers of GlobeRanger, that the Defendants had developed the Navy RFID Solution. Software AG and Naniq used these misrepresentations and false attributions to gain an unlawful competitive advantage over GlobeRanger, destroy GlobeRanger's reputation among customers and peers, and damage GlobeRanger's dominant market position in the government sector. And they did it right in GlobeRanger's backyard in Dallas, Texas.

88. As the sponsor of the summit, Software AG key personnel such as Software AG Sr. Vice President and General Manager Bruce Williams and Dave Brooks, Software AG Senior Director, moderated, presented, and worked the crowd.

89. Software AG's stolen RFID Solution was showcased in Kim Gray's presentation "Navy AIT & Asset Visibility Efforts: A Comprehensive Plan Forward." Kim Gray and Software AG falsely represented that the Navy's passive RFID system was "the only [passive] RFID enterprise system in industry today," when in fact GlobeRanger was deployed across a large spectrum of enterprises, and had been operating enterprise-wide, with multiple

commendations, at the DLA for years. Software AG and Ms. Gray sought to mislead prospective and current customers and peers of GlobeRanger that Software AG was on top in passive RFID systems for the government, when in fact the Marine Corps and Army were in the process of adopting GlobeRanger, not Software AG, at that time, and Software AG had only obtained their contract through unlawful means and at great expense to our service members.

90. Software AG had used the Navy to steal a passive RFID Solution from GlobeRanger for commercial gain. On the conference agenda, available on Software AG's 2010 Dallas Supply Chain Conference website at http://dallas.supplychainsummit2010.com/, Software AG used the Navy once more, falsely representing Kim Gray as "Kim Gray, Compliance Officer, U.S. Navy," when in fact Kim Gray is not an employee of the U.S. Navy and does not represent the U.S. Navy.

91. Software AG – Germany directed and controlled this false marketing effort. Software AG even uploaded a version of her presentation on to the Software AG – Germany website,[2] seeking to encourage more business from their wrongful and fraudulent acquisition of GlobeRanger's trade secrets.

92. There was a deliberate effort by Defendants to misappropriate the proprietary, confidential and trade secret information of GlobeRanger through improper means and use this information to knock GlobeRanger out of its superior market position in the government passive RFID market and to enrich Defendants. Further, the Defendants and their co-conspirators misappropriated the proprietary, confidential and trade secret information of GlobeRanger in direct violation of GlobeRanger's EULA provisions. The length of time that this has been ongoing and the continued, ongoing involvement of Defendants indicate that this is a deliberate,

[2] All internet traffic for the U.S. Subs and webMethods is automatically redirected to Software AG – Germany's website.

determined action amongst all of the parties. The admission – and laughter following – the admission of the theft show that the Defendants were acting with malicious intent. As a result of their unlawful conduct, Defendants gained a proprietary advantage with respect to the Navy AIT contract, government RFID contracts and the RFID market in general.

V. CAUSES OF ACTION

COUNT I – MISAPPROPRIATION OF TRADE SECRETS

93. Plaintiff incorporates by reference the allegations of all preceding paragraphs as if fully set forth herein.

94. Plaintiff owned certain trade secrets, including but not limited to its architecture, business processes and software.

95. Defendants used or disclosed such trade secrets in violation of a confidential or contractual relationship with Plaintiff, after acquiring the trade secret by improper means, or after acquiring the trade secret with notice that the disclosure was improper.

96. Defendants' tortious conduct is a direct and proximate cause of damages to Plaintiff.

97. Plaintiff is further entitled to exemplary damages pursuant to Texas Civil Practice & Remedies Code § 41.003(a), as the harm with respect to which it seeks recovery results from the fraud, malice, and/or gross negligence of Defendants.

COUNT II – UNFAIR COMPETITION

98. Plaintiff incorporates by reference the allegations of all preceding paragraphs as if fully set forth herein.

99. Defendants committed an illegal or wrongful act in competition with Plaintiff which interfered with Plaintiff's ability to conduct its business.

100. Defendants' tortious conduct is a direct and proximate cause of damages to Plaintiff.

101. Plaintiff is further entitled to exemplary damages pursuant to Texas Civil Practice & Remedies Code § 41.003(a), as the harm with respect to which it seeks recovery results from the fraud, malice, and/or gross negligence of Defendants.

COUNT III – CONSPIRACY

102. Plaintiff incorporates by reference the allegations of all preceding paragraphs as if fully set forth herein.

103. Defendants entered into a combination to engage in fraud against Plaintiff for their own personal gain. Defendants had a meeting of the minds with respect to those unlawful purposes and committed one or more overt acts to further the conspiracy.

104. Defendants' tortious conduct is also a direct and proximate cause of damages to Plaintiff.

105. Plaintiff is further entitled to exemplary damages pursuant to Texas Civil Practice & Remedies Code § 41.003(a), as the harm with respect to which it seeks recovery results from the fraud, malice, and/or gross negligence of Defendants.

COUNT IV – TORTIOUS INTERFERENCE

106. Plaintiff incorporates by reference the allegations of all preceding paragraphs as if fully set forth herein.

107. Plaintiff had a valid contract(s) with Navy AIT, including but not limited to the EULA.

108. Defendants willfully and intentionally interfered with the contract(s), without privilege to do so.

109. Plaintiff incurred actual damage or loss due to breach of the contract(s).

110. Defendants' tortious conduct is also a direct and proximate cause of damages to Plaintiff.

111. Plaintiff is further entitled to exemplary damages pursuant to Texas Civil Practice & Remedies Code § 41.003(a), as the harm with respect to which it seeks recovery results from the fraud, malice, and/or gross negligence of Defendants.

COUNT V – PERMANENT INJUNCTION

112. Plaintiff incorporates by reference the allegations of all preceding paragraphs as if fully set forth herein.

113. SAG is in possession of GlobeRanger's trade secrets. GlobeRanger requests a permanent injunction to restrain SAG, its parents, affiliates, and successors, and assigns from using or disclosing GlobeRanger's trade secrets by any means, including displaying, marketing, selling, transferring, distributing, or prepare derivative works of the products, modules, and adapters comprising the SAG Solution, including, but not limited to webMethods, WmSockets, WmAlienRFID, RFID Business Process, Analytics, User Interfaces, RFID Fixed Reader Integration, RFID Printing, RFID Edge, Handhelds, and RFID Partner Integration, and any extensions, adaptations, or modifications to the foregoing.

VI. PRAYER

WHEREFORE, Plaintiff GlobeRanger Corporation requests that the Court issue judgment against Defendants Software AG, Software AG USA, Inc., Software AG, Inc., Naniq Systems, LLC and Main Sail LLC on all counts, and award it:

a. Actual damages resulting from Defendants' conduct;

b. Incidental, consequential, and exemplary damages, as permitted by law;

c. Injunctive relief as specified herein;

d. Pre-judgment and post-judgment interest as provided by law;

e. Attorneys' fees and costs, as permitted by law; and

f. Such other and further relief, at law or in equity, to which it may be justly entitled.

DATED: August 20, 2014

Respectfully submitted

/s/ Ophelia F. Camiña
Ophelia F. Camiña
State Bar No. 03681500
David D. Shank
State Bar No. 24075056
SUSMAN GODFREY L.L.P.
901 Main Street, Suite 5100
Dallas, TX 75202
Phone: 214.754.1910
Fax: 214.754.1933

Brian D. Melton
Texas Bar No. 24010620
Katherine H. Kunz
Texas Bar No. 24083337
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002-5096
Phone: 713.651.9366
Fax: 713.654.6666

Attorneys-in-Charge for
GLOBERANGER CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on 20th day of August, 2014, a true and correct copy of the foregoing document was submitted to the Clerk of the Court of the U.S. District Court, Northern District of Texas, using the CM/ECF system, and was served upon all counsel that have appeared in this case through this Court's electronic filing system.

/s/ Ophelia F. Camiña
Ophelia F. Camiña